claim encompasses the features of generating a second identifier as a function of the random number from at least a portion of the first identifier and from the result of executing the asymmetrical algorithm and the symmetrical algorithm, storing the second identifier, and transmitting the second identifier to a server each time the terminal identifies itself to the server.

Contrary to the Examiner's assertions, the combination of *Aura, Owada*, and *Kang* fails to disclose or suggest the aforementioned features.

As discussed in the previous response, *Aura* discloses an identity protection technique in which a mobile station inputs a public key (Kd key) and an identifier (IMSI) to an algorithm to generate an encrypted identity. *See* Aura, col. 5, lines 9-12. The public key is generated by inputting a random number and private key (Kh key) into a hash function. Id., col. 4, lines 45-49. The encrypted ID and the random number are sent to a home location register HLR. The identifier data of the subscriber is always encrypted using a fresh, not-previously-used random number, so the network is unable to make a connection between the encrypted identities of the user. Id., col. 5, lines 28-32. As a result, *Aura* does not disclose nor has a need to store the identifier for future identifications.

The Examiner relies on *Owada* to remedy the deficiencies of *Aura* as it concerns using asymmetrical and symmetrical algorithms in generating the second identifier.

Owada discloses a security technique in which, to encode data, a storage medium generates a random number, which is then used as a symmetrical key to encode information. *See* Owada, pgph [0043]. The random number (symmetrical key) is asymmetrically encoded with a public key (asymmetrical key). Id., pgph

[0044]. The encoded information and the encoded random number are sent to a general purpose processing device for storage (emphasis added). *See* Id., pgph [0045]. Because the general purpose processing device cannot decode the second symmetrical key, this device cannot use the stored information. Id., pgph [0046]. When the storage medium requests a transfer of the data from the general processing device, the storage medium receives the encoded information and the encoded key from the general processing device. Id., pgph [0051]. The storage medium decodes the encoded random number using a private key (2nd asymmetrical key). Id., pgph [0051]-[0052]. The decoded random number (symmetrical key) is then applied to an algorithm to decode the information. Id., pgph [0052].

Applicant acknowledges that *Owada* discloses the use of both an asymmetric and symmetric algorithm. However, the encrypted information generated by *Owada* is not identification data. Rather the encrypted information is data that one storage medium is sending to another storage device or a general processing device for storage. When the storage medium chooses to use the data stored in the other device it sends a request to the other device, and executes a decryption algorithm on the received encrypted data. There is nothing in *Owada* that would have disclosed or suggested to one skilled in the art that this encryption/decryption and storage technique can be implemented in *Aura* with respect to the identification technique of *Aura*. In fact, *Aura* teaches away from the storage of a random number as is taught by *Owada*.

Kang is alleged to remedy the deficiencies of *Aura* and *Owada* as it concerns storing a second identifier in the memory of the terminal resource and using the

second ID each time the terminal resource identifies itself to the server, which features are encompassed in Applicant's independent claims. *Kang* discloses a method and device that protects the content transmitted between mobile phones. During this process, several memory devices between a first mobile phone in the transmission and the second mobile phone in the transmission are used. These memory devices do not store an identifier or a second identifier as alleged by the Examiner, but merely disclose that each of the memory devices stores a key used to either encode or decode content subject to a protection request (Fig. 3; paragraphs 46-50). There is nothing in *Kang* that would have guided one skilled in the art to believe that this document discloses storing a second identifier, and transmitting the second identifier to a server each time the terminal identifies itself to the server, as is recited independent claims 1, 3, 4, 8, and 10. Thus, *Kang* fails to remedy the deficiencies of *Aura* and *Owada*.

In summary, *Aura*, *Owada*, and *Kang* when applied individually or collectively fail to disclose or suggest each feature and/or the combination of features recited in Applicant's claims. For at least these reasons, withdrawal of the rejection under 35 U.S.C. §103 is respectfully requested.

CONCLUSION

Based on the foregoing amendment and remarks, Applicant respectfully submits that claims 1-11 and 13-16 are allowable and this application is in condition for allowance. Favorable examination and consideration of this application are respectfully requested. In the event any unresolved issues remain, the Examiner is invited to contact Applicant's representative identified below.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: March 28, 2011

By: /Shawn B. Cage/
Shawn B. Cage
Registration No. 51522

Customer No. 21839
703 836 6620